

Communication Systems and System Support

1. Basic Telephone Support.....	Page 3
2. Local Area Network/Wide Area Network Connectivity (LAN/WAN).....	Page 5
3. Terminal Server Access Controller System (TSACS).....	Page 6
4. Telephone Toll Charges.....	Page 7
5. Telephone Work Orders.....	Page 8
6. Virtual Private Network (VPN).....	Page 9
7. Trunked Radio System.....	Page 11

Visual Information Processes

AVI.....	Page 12
----------	---------

Document Management

Copier Management.....	Page 13
------------------------	---------

Information Assurance

1. IA.....	Page 14
2. Department of Defense Information Technology Security Certification and Accreditation Process.....	Page 16

Automation

1. E-Mail ARMY Active Directory.....	Page 18
2. ARMY Active Directory E-Mail Additional Storage.....	Page 19
3. ARMY Blackberry/Personal Digital Assistant (PDA) Services.....	Page 20
4. Shared Use Server Home (H) and Public (P) Drives.....	Page 21
5. Shared use Server Hosting-Additional Storage.....	Page 23
6. Single Use Server- Level 1.....	Page 24
7. Single Use Server – Level 2.....	Page 25
8. Single Use Server – Level 3.....	Page 26
9. E-Server.....	Page 28
10. Customer Support Center (CSC) Services.....	Page 29
11. Customer Support Center (CSC) MPMC Services.....	Page 31
12. Patch Management.....	Page 34

FY 2006
Supplier and Receiver Clauses

13. Secret Internet Protocol Router NETwork (SIPRNET).....	Page 35
14. SQL/FileMaker Application.....	Page 36
15. Automated Time Attendance and Production system (ATAAPS Support).....	Page 38
16. Web Services - Level 1 Site Hosting.....	Page 40
17. Web Services – Level 2 Site Hosting.....	Page 41
18. Web Services _ Level 3 Site Hosting.....	Page 42
19. Web Services - Other (WEB Development).....	Page 43
20. Customer Account Manager (CAM) and Project Management Support.....	Page 45
21. Application Support for General Use and Legacy Systems (ISMs).....	Page 46
22. DBA Support – Oracle.....	Page 48

Communication Systems and Systems Support

Basic Telephone Support

Description of Services: Fort Detrick DOIM provides basic telephone support to Fort Detrick customers. Support includes subscriber service for long distance, Defense Switched Network, and commercial phone service. Both voice and data circuits (for facsimile machines and modem connections) and equipment (telephone handsets) are provided. Charges for toll calls and work orders for new equipment, repairs, or installations are outside of the SLS (Standard Level of Service) and are billed accordingly.

Supplier will:

- a. Provide subscriber service to include access to long distance, DSN and commercial phone service.
- b. Procure dedicated voice and data circuits, and phones (equipment).
- c. Voice Switching: Provide single line telephone service to each user at the current rate. This includes a touch tone telephone and at least Class C Service (AR 25-1, Section 6.3C). Meet 98% reliability (as defined in IT Metrics); provide average 90% success rate on local (off-post); provide access to Integrated Services Digital Network (ISDN), Federal Telecommunications System (FTS), Defense Switched Network (DSN) for CONUS, OCONUS, and local trunks. Post telephone operator support will be provided (0730 – 1630) Monday thru Friday.
- d. Provide voice mail services and maintain an installation phone book (electronically). * See note at end of this section.
- e. Provide Trunked Radio System-Infrastructure (Users must provide own connection equipment).
- f. Non-Tactical Trunked Radios (NTTR): Provide separate narrow band digital trunking for firefighting, ambulance/emergency medical, law enforcement, environmental, garrison operations, and range control organizations to include maintenance of infrastructure. Meet 95% reliability (as defined in IT Metrics), 95% access, and 98% coverage.
- g. Provide special circuits for fire alarms, intrusion alarms in arms rooms, and other safety/security systems specifically directed by DA or local regulation.

Receiver will:

- a. Make requirements known to Supplier.
- b. Request services and support by providing necessary request and/or documentation.
- c. Alert the Supplier as soon as possible on issues or problems that arise.
- d. Provide the Supplier ten working days advance notice to implement new service.

FY 2006
Supplier and Receiver Clauses

- e. Provide the supplier with appropriate pertinent information necessary when requesting new user account.

*** Note:** ISDN does not include VTC. VTC services are carried through an ISDN (telephone service). All ISDN installations which are part of a VTC service will be done by Verizon or by the Mednet System (If your organization supports the medical services) as a normal telecommunications install and will follow normal procurement process by going through the Fort Detrick DOIM Telecommunications Specialist. Fort Detrick DOIM will handle these as a one-time charge for ISDN installation services.

The monthly recurring charges for VTC service and ISDN will be billed directly from the vendors and are independent of the Fort Detrick DOIM Service Level Agreement (SLA). The charges might include per minute charges and monthly fees. Those items and other third-party charges are the responsibility of the recipient organization to pay directly to the vendor.

Local Area Network/Wide Area Network Connectivity (LAN /WAN)

Description of Services: Fort Detrick DOIM provides connectivity over the LAN to the WAN. This support includes all bandwidth usage costs to support the Fort Detrick installation. A WAN is a communications network that covers a broad geographic area, such as a province, state, or country. A LAN is contained within a building or complex. IP addresses include both network desktops and printers connected to the LAN.

Supplier will:

- a. Provide connection to the NIPRNET and Internet.
- b. Provide WAN/LAN switch management.
- c. Apply all security rules to Fort Detrick DOIM -owned Government Furnished Equipment (GFE).
- d. Provide most recent Army-approved virus protection to GFE (only if owned by Fort Detrick DOIM).
 - 1 Data Networks.
 - 2 Provide 100Mbps (or greater) unclassified and classified (for required systems), connectivity to all required End User Buildings on the installation.
 - 3 Provide WAN access to support electronic mail, web browsing, and Standard Army Systems and DOD Installation Support Modules.
 - 4 Provide remote dial-in service. Access will be provided via GFE only, not by a user's personal equipment.
 - 5 Provide secure access to Fort Detrick Local Area Network (LAN) using VPN. Access will be provided via GFE only, not by user's personal equipment.
 - 6 If funded: provide for Continuity of Operations Services for critical portions of the Installation Level Network and DOIM Network Operations Center.

Receiver will:

- a. Apply most recent Army-Approved virus protection to LAN hardware (Routers/Switches/Hubs, etc.) not managed by the Fort Detrick DOIM and inform DOIM IA when virus updates are complete.
- b. Provide funds to Supplier to connect TO NIPRNET and/or Internet
- c. Provide funds to Supplier to connect Receiver building(s) to the LAN
- d. Provide funds to Supplier for Switch maintenance.
- e. NOT be permitted to share user authentication information
- f. NOT be permitted to use GFE for non-government work
- g. NOT be permitted to use personal equipment to connect to government resources.
- h. Abide by Fort Detrick DOIM guidelines before acquiring hardware/software that will use the LAN
- i. Only use TCP/IP base protocol
- j. Furnish funds to purchase switches, to include cable patches, in order to connect users to the LAN

Terminal Server Access Controller System (TSACS)

Description of Services: Fort Detrick DOIM provides TSACS access for dial-up modem connectivity to the Internet. The TSACS system is accessible worldwide. Both Continental United States (CONUS) or Outside Continental United States (OCONUS) users can use TSACS to access the Internet remotely and e-mail applications through a secure network.

Supplier will:

- a. Provide TSACS (Dial-up modem connections).
- b. Provide hardware which the user will connect to through the use of modems while TDY or working off post from Fort Detrick.
- c. Provide security requirements, operational guidelines, and user authentication.

Receiver will:

- a. Provide Government Furnished Equipment (GFE) for connection to Fort Detrick TSACS Server via modems.
- b. Use TSACS for official Government business only
- c. Run latest Anti-Virus software/latest security updates
- d. NOT share user authentication information
- e. Provide telephone connection to use as transport media when connecting to Fort Detrick TSACS.
- f. Have GFE scanned for vulnerabilities according to local security policy.
(EXAMPLE: quarterly)
- g. Recognize that a TSACS connection establishes the remote equipment as an extension of the Fort Detrick Network Infrastructure subject to all US Government, DOD, DA, Fort Detrick, and organizational rules and regulations that apply to hardware, software, and use of those Network facilities.

FY 2006
Supplier and Receiver Clauses

Telephone Toll Charges

Description of Services: Fort Detrick DOIM provides basic telephone support to Fort Detrick customers. Charges for toll calls and work orders for new equipment, repairs, or installations are outside of the standard level of service (SLS) and are billed accordingly.

Supplier will:

- a. Provide subscriber service to include access to long distance, DSN and commercial phone service.
- b. Provide dedicated voice and data circuits, and single line phones.

Receiver will:

Provide payment for all long distance toll charges submitted in the monthly TCO report.

FY 2006
Supplier and Receiver Clauses

Telephone Work Orders

Description of Services: Fort Detrick DOIM provides basic telephone support to Fort Detrick customers. Charges for toll calls and work orders for new equipment, repairs, or installations are outside of the SLS and are billed accordingly.

Supplier will:

- a. Procure dedicated voice and data circuits, and single line phones.
- b. Perform requested work (new install, repair, move, etc.) within 10 working days.

Receiver will:

- a. Provide payment for all telephone work order charges as invoiced.
- b. Be responsible for providing funds to Fort Detrick DOIM necessary to cover costs for installation of new LAN drops from user's work area to the Communications Closet.
- c. Safeguard equipment from misuse and damage.
- d. Provide supplier a minimum of 10 working days in advance notice of new equipment requirements or line moves.

Virtual Private Network (VPN)

Description of Services: Fort Detrick DOIM provides VPN secure access to the Fort Detrick Local Area Network (LAN). A VPN provides a means for a Fort Detrick user of Ft. Detrick services to access the services from a remote location over a secure channel. This is done with a method of authenticating the user and encapsulating the data as it traverses the network, allowing it to bypass most access lists. The access method used is independent of the VPN service. The base access method might be TSACS, a cable service from a local provider, or some other dial-up method. VPN is a security augmentation to the base access method. User authentication identifies the user to the VPN service provider. By encapsulating user data it is “sealed”, so it passes across the networks between the users’ PC and the VPN service provider without causing harm or being interrupted along the way. In effect the VPN service provider is vouching for the user and the users’ network activities.

Supplier will:

- a. Engineer and operate a VPN environment supported by hardware and software that will permit authorized users to access their Fort Detrick Network Infrastructure resources from approved remote locations and authorized equipment; maintain a list of any disapproved Internet Service Providers based on ACERT or other official advisories; issue, manage, and maintain VPN accounts and authorizations; and implement and configure required hardware and/or software for the approved remote equipment.
- b. Perform a security scan of the Receiver personal computer
- c. Provide VPN account
- d. Provide VPN Client
- e. Provide hardware which the user will connect to through the use of broadband or dial-up access while TDY or working off post from Fort Detrick
- f. Provide security requirements, operational guidelines, and user authentication.

Receiver will:

- a. Provide Government Furnished Equipment (GFE) for connection to Fort Detrick LAN via VPN.
- b. Make pc available to the Supplier for security scan and installation of the VPN client.
- c. Arrange for reimbursement of the Fort Detrick DOIM for the cost of services provided.
- d. Designate authorized users and coordinate with the Fort Detrick DOIM Information Support Division for the implementation and configuration of required hardware and/or software to support authorizations.
- e. Use VPN for official Government business only.
- f. Run latest Anti-Virus software/latest security updates
- g. NOT share user authentication information

FY 2006
Supplier and Receiver Clauses

- h. Select and arrange for payment of acceptable Internet Service Provider (ISP).
- i. Install, manage, and maintain any software or hardware required by the ISP for access.
- j. Have GFE scanned for vulnerabilities according to local security policy according to local security policy. (EXAMPLE: quarterly)
- k. Coordinate through the Fort Detrick DOIM Customer Support Center (CSC) for installation and configuration of VPN hardware and/or software on approved remote equipment subsequent to verification of correct operation of services from the ISP.
- l. Recognize that the VPN establishes the remote equipment as an extension of the Fort Detrick Network Infrastructure subject to all US Government, DOD, DA, Fort Detrick, and organizational rules and regulations that apply to hardware, software, and use of those Network facilities.

Trunked Radio System

Description of Services: Fort Detrick DOIM provides trunked radio support to Fort Detrick customers that include subscriber service local and long distance within the National Capital Region's (NCR) trunked radio system coverage path. Charges for work orders for new equipment, radio repairs, or installations are outside of the SLS and are billed accordingly.

Supplier will:

- a. Provide Trunked Radio System-Infrastructure (Users must provide own connection equipment).
- b. Non-Tactical Trunked Radios (NTTR): Provide separate narrow band digital trunking for firefighting, ambulance/emergency medical, law enforcement, environmental, garrison operations, and range control organizations to include maintenance of infrastructure. Meet 95% reliability (as defined in IT Metrics), 95% access, and 98% coverage.

Receiver will:

Provide necessary connection equipment.

Visual Information Processes

Audio Visual Information (AVI)

Description of Services: Fort Detrick DOIM Visual Information (VI) provides photography, audiovisual, graphics and limited printing services to Fort Detrick customers. Services needed outside of normal business hours require reimbursable overtime, unless other arrangements have been made. No overtime service will be provided until VI receives written authorization from an approving officer with the requesting unit.

Supplier will:

Provide Photography services to include

- a. Official DA photos and ceremonies. (*Promotions, reenlistment, change of commands, awards, etc.*)
- b. Studio and field photography services
- c. Hard copy and/or digital prints

Provide AudioVisual services to include

- a. Official ceremonies and training exercises at Battalion level and above.
- b. Edit and produce master tape(s)
- c. Audio and video duplication
- d. Equipment loan
- e. Set up and operation of equipment

Provide Graphics services to include

Design and layout (*Flyers, slides, programs, brochures, etc.*)

Provide Printing services to include

- a. Black and white and color reproduction (*Posters, flyers, banners, programs, brochures*)
- b. Special stock and/or material (*Parchment, envelopes, laminating material, etc.*)

Receiver will:

- a. Make requirements known to Supplier
- b. Request services and support by providing necessary request and or documentation
- c. Submit service requests with sufficient lead time to prepare

Document Management

Copier Management

Description of Services: The DOIM can provide digital copiers on a cost reimbursable basis. Three models are available to support low, medium, and high quantity workload. Four popular options that expand the copier's capabilities are also available for a one-time cost. These options enable the copier to function as a fax, handle classified reproduction, operate as a stand alone scanner, and expand document finishing capabilities. All three models offer network printing and scanning as part of the basic capability. In addition, the DOIM offers help desk support for both toner replacement and copier problems. Customers are responsible for replacing the toner, but the help desk will deliver spares to the worksite. When there is a problem with the copier, customers call the help desk and they either help resolve the problem or pass it on to the vendor. Copiers are provided via an IDIQ contract and are purchased under a three year lease-to-own program. Therefore, customers must agree to a three year funding commitment and provide funds on an annual basis.

Supplier will:

Upon receipt of funding provide copier and support.

Receiver will:

- a. Agree to a three year funding commitment and provide funds on an annual basis.
- b. Appoint a key operator and alternate. (Key Operator Memo details responsibilities)
- c. Coordinate all service and modifications with the DOIM.

Cost basis for reimbursement:

Pricing is per model and options selected.

Information Assurance

(IA)

Description of Services: Our sole mission is to protect and defend network availability, protect data integrity, and provide the ability to implement effective computer network defense for the Fort Detrick Network. The threat to telecommunications and IS throughout the Army is genuine and expanding. The increasing number of information resources result in an increased vulnerability to threats caused by both authorized users and through external attack. The reliance on information systems has made information technology a competitive weapon of unparalleled power and importance. The Department of Defense (DoD) has identified information and information resources as a priority target in future conflicts. As such, the simultaneous defense of our own information resources considered is just as critical. Therefore, it is the responsibility of all users to maintain Army operating standards and report any suspicious activities.

Supplier will:

- a. Coordinate the detection, correction, and reporting of malicious and unauthorized activities.
- b. Implement and manage the Information Assurance Vulnerability Management (IAVM) program for all installation and tenant activities.
- c. Perform network or workstation scans and compile vulnerability reports and corrections.
- d. Provide written Certification and Accreditation statements (for example, Interim Approval to Operate/Connect (IATO/IATC)), and formal approval to operate (ATO) Certification and Accreditation documentation after formal review of SSAA and Certification and Accreditation documentation.
- e. Develop and coordinate implementation of security procedures and protocols governing network operations.
- f. Assist in the formal Information Assurance (IA) certification programs for Network Managers and Systems Administrators Information Technology Professionals; training for scanning personnel; and IA workstation/server implementation training/guidelines.
- g. Implement and manage the IAVA program for all installation and tenant activities.

Receiver will:

Army tenant units or activities must comply with the IA requirements of both their parent MACOM and the supporting installation. Army and non-Army tenant operations must comply with the host installation's IA policy if they connect to the installation's information infrastructure. Army tenant units or activities and units based in or under operational control (OPCON) of a MACOM other than their parent MACOM will comply with the IA requirements of both parent and host MACOMs. If a non-Army tenant uses any part of the host installation infrastructure, the installation IAM will

FY 2006
Supplier and Receiver Clauses

require the use of configuration management controls consistent with the installation's information management and configuration management process. All tenant activities will —

- a. Identify and coordinate all system upgrades, fieldings, pilots, tests, and operations of new or upgraded systems with the installation IAM, DAA, and DOIM.
- b. Identify ISS and provide the approved Certification and Accreditation documentation to the installation IAM.
- c. Support installation IA efforts and requirements, and identify constraints in sufficient time to permit coordination and preparation of a viable IS security solution.
- d. Coordinate and conduct vulnerability assessments or compliance scanning, and report completion and results as required.

***Department of Defense Information Technology Security Certification
and Accreditation Process (DITSCAP)***

The Ft Detrick DOIM provides a Certification and Accreditation service for tenants. For the DoD tenants, the DITSCAP process is followed. For non-DoD tenants, the process to be followed will vary but the DOIM is capable of using any Federal agency Certification and Accreditation process.

The service offered will be highly customizable depending on the needs of the tenant organization. The primary factors that lead to this variability are the tenant's availability, willingness, and ability to participate in the process, their budget constraints, and their knowledge of the Certification and Accreditation process itself.

Supplier will:

- a. Ensure proper Certification and Accreditation based on systems environment, sensitivity levels, and security safeguards in accordance with this regulation and the DODI 5200.40 (DITSCAP).
- b. Provide a certification agent (CA) with installation-wide Appointment Orders. CA will:
 - o Evaluate the technical and non-technical security features for IA C and A.
 - o Ensure that security testing and evaluation is completed and documented.
 - o Advise the DAA on the use of specific security mechanisms.
 - o Provide Certification and Accreditation documentation to the DAA.
 - o Assess changes in the system, its environment, and operational needs that could affect the accreditation.
 - o Include CSLA personnel as a cryptographic advisor on certification teams.
- c. Provide written Certification and Accreditation statements (for example, Interim Approval to Operate/Connect (IATO/IATC)), and formal approval to operate (ATO) Certification and Accreditation documentation after formal review of SSAA and Certification and Accreditation documentation.
- d. Provide Phase IV DITSCAP continued information assurance management as required

Receiver will:

- a. Provide an inventory of equipment to be included within the DITSCAP boundary.
- b. Provide the final DITSCAP documentation to the DOIM Information Assurance Manager (IAM), ready for certification, before the system is submitted for approval to operate.
- c. Identify any activity to which the system will have connectivity requiring a Security Memorandum of Agreement to operate.

FY 2006
Supplier and Receiver Clauses

- d. Indicate whether they require life cycle information assurance support, DITSCAP Phase IV, for their system.

Automation

E-mail ARMY Active Directory

Description of Services: Fort Detrick DOIM provides electronic mail accounts using Microsoft Active Directory (AD) Mail for Army customers. Microsoft Active Directory is an e-mail server that can be used to handle official government e-mail. It can also be configured to send and receive outgoing mail on demand. Service includes maintaining the e-mail infrastructure and troubleshooting issues to insure e-mail is delivered in a timely fashion.

Supplier will:

- a. Provide email services to include host support and accounts management.
- b. Provide 50 MB mail storage per user.
- c. 24x7 operation (with 3 hours bi-weekly scheduled for preventive maintenance)
- d. Achieve e-mail server availability of 99% (24x7), excluding scheduled maintenance.
- e. Add/delete users within 1 working day of request by Receiver IAW established security procedures after receiving request from the Customer Support Center (CSC)
- f. Perform mail server Service Pack updates
- g. Perform mail server Antivirus updates
- h. Perform full system and incremental backup per prescribed schedules and processes.
- i. Restore mailboxes upon request from Receiver via the CSC within 48 hours after receiving request.
- j. Provide password security by facilitating password change per AR 25-2.

Receiver will:

- a. Make requirements known to Supplier.
- b. Alert the Supplier as soon as possible regarding issues or problems as they arise.
- c. Request services and support by providing necessary request and or documentation.
- d. Supply forty-eight hours advance notice when requesting a mailbox move.
- e. Provide the Supplier one week advance notice with the appropriate approval when requesting forwarding of user mailbox to another location.
- f. Alert Supplier immediately when a user departs or changes duty station in order to remove any e-mail referencing the user account.
- g. Provide the Supplier forty-eight hours to restore a user mailbox.
- h. Utilize Government e-mail and all its components for official business only.

Army Active Directory E-mail – Additional Storage

Description of Services: Fort Detrick DOIM can provide additional electronic storage for Army customers using Microsoft Active Directory email.

Supplier will:

- a. Provide e-mail services, including host support and accounts management.
- b. Provide 50 MB additional mail storage per user.

Receiver will:

Provide payment, as invoiced, for e-mail storage capacity utilized in excess of SLS inclusion in blocks of 50 MB of additional storage.

Army Blackberry/Personal Digital Assistant (PDA) Services

Description of Services: The Fort Detrick DOIM provides Blackberry Enterprise Server (BES) to Army customers to allow secure access to the Fort Detrick email via the Blackberry wireless communication devices. This service will allow user access to email within the Blackberry wireless network coverage area.

Supplier Will:

- a. Supplier will maintain Blackberry Enterprise Server (BES)
- b. Supplier will test software updates.
- c. Supplier will provide Receiver with Standard Operating Procedures on each Blackberry device utilized by customer.
- d. Supplier will provide Receiver 4 hour response to Blackberry issues or requests after being notified by the CSC of a request for service

Receiver Will:

- a. Make requirements known to Supplier
- b. Request services and support by providing necessary request and or documentation
- c. Receiver will notify the Supplier as soon as possible on issues or problems that arise
- d. Receiver will provide Supplier with Blackberry Enterprise Server licenses.
- e. Receiver will provide Supplier with Itrezzo software to receive attachments from email.
- f. Receiver will provide wireless airtime to include phone support maintenance contract.
- g. Receiver will supply all Blackberry devices necessary for users to utilize wireless network capabilities.
- h. Receiver will use the Blackberry for official Government business only.

***Shared Use Server Home (H)
And Public (P) Drives***

Description of Services: Fort Detrick DOIM provides server-hosting support for Shared Servers by way of providing users with 1 GB of electronic storage on the Home (H) and Public (P) drive. This service includes providing users with access to print servers and access to public drive space. The DOIM provides the server hardware, software and operating system. Monitoring and support are provided on a 7 x 24 coverage with after hours on call staff in the event of an outage. Scheduled maintenance will be performed within the window of 8:00-12:00 am EST on Sundays unless critical requirements force an immediate unscheduled downtime to provide corrective resolutions.

Supplier will:

- a. Provide Server Hosting services for shared servers on-site at Fort Detrick DOIM (administration, back-up, and data storage) to include:
- b. Provide 1 GB of storage capacity per account.
- c. Monitor, coordinate, and administer server resources.
- d. Maintain the availability of the server(s) to its users on a 24 x 7 basis with a goal of 98% availability each year.
- e. Advise and assist users regarding access to the server(s).
- f. Establish and perform system backup procedures and documentation.
- g. Implement a comprehensive information security program per AR25-2, Army and MEDCOM regulations to include physical security procedures.
- h. Use fault management techniques designed to diagnose problems and provide timely solutions.
- i. Monitor the user environment, including login scripts, menu creation, and directory structure, as needed.
- j. Perform regularly scheduled evaluation and maintenance of all components (i.e. file servers, and print servers,), including preventive maintenance.
- k. Provide around the clock monitoring and repair of system operations.
- l. Implement approved and planned changes to the LANs and document configuration changes.
- m. Inform the user community of planned maintenance schedules and planned outages.

Receiver will:

- a. Make requirements known to Supplier
- b. Request services and support by providing necessary request and or documentation
- c. Alert the Supplier as soon as possible on issues or problems that arise

FY 2006
Supplier and Receiver Clauses

- d. Provide the supplier with appropriate pertinent information necessary when requesting new user account
- e. Provide the Supplier forty-eight hours advance notice when requesting data transfer
- f. Notify the supplier immediately when a user departs or changes duty station in order to remove any data referencing user account
- g. Provide the Supplier twenty-four hour advance notice to restore user data
- h. Use shared network server storage and all its components for official government business only.

Shared Use Server Hosting – Additional Storage

Description of Services: Fort Detrick DOIM provides server-hosting support for Shared Servers. These servers contain programs that collectively serve the needs of the entire organization, a single user, department, or specialized application. A shared server is both the computer hardware and its main software, the operating system.

Supplier will:

- a. Provide Server Hosting services for shared servers on-site at Fort Detrick DOIM Building 1422
- b. Provide 1 GB additional storage capacity per account

Receiver will:

Provide payment, as invoiced, for shared use server hosting storage capacity utilized in excess of SLS inclusion in blocks of 100 MB of additional storage.

Single Use Server-Level 1

Description of Services: The Fort Detrick DOIM provides state-of-the-art computer room facility services for Servers which are on the property book of a Tenant organization. These servers contain programs that collectively serve the needs of the entire organization, a single user, department, or specialized application. The tenant organization provides all support for these servers as they deem necessary.

Supplier will:

- a. Provide an environmentally controlled facility to host servers to include floor space, power, and air conditioning.
- b. Provide physical security for the servers located in the DOIM from the aspect of being in a locked and controlled facility
- c. Recommend to the Receiver guidelines and regulations to follow to ensure staff providing support to the Receivers server(s) are following ARMY and MEDCOM regulations per AR25-2

Receiver will:

- a. Make requirements known to Supplier
- b. Request services and support by providing necessary request and or documentation
- c. Alert the Supplier as soon as possible on issues or problems that arise
- d. Maintain the availability of the server(s) to its users
- e. Establish and perform system backup procedures and documentation.
- f. Implement a comprehensive information security program per AR25-2, MEDCOM, Army or higher Command guidelines and physical security procedures.
- g. Use fault management techniques designed to diagnose problems and provide timely solutions.
- h. Monitor the user environment, including login scripts, menu creation, and directory structure, as needed.
- i. Perform regularly scheduled evaluation and maintenance of all components (i.e. file servers, and print servers), including preventive maintenance.
- j. Provide backup and COOP for all Servers.

Single Use Server Hosting-Level 2

Description of Services: Fort Detrick DOIM provides server-hosting support for Single Use Servers. These servers contain programs that collectively serve the needs of the entire organization, a single user, department, or specialized application. These servers are provided to the DOIM by the customer. The customer is responsible for hardware and software maintenance on these servers. The DOIM can obtain maintenance for the customer on a reimbursement basis. In this usage, a server is both the computer hardware and its main software, the operating system.

Supplier will:

- a. Maintain the availability of the server(s) to its users.
- b. Establish and perform system backup procedures and documentation to include storage of backup media and DR drives at a remote COOP site.
- c. Implement a comprehensive information security program per AR25-2, ARMY and MEDCOM guidelines and physical security procedures.
- d. Use fault management techniques designed to diagnose problems and provide timely solutions.
- e. Provide technical staff that are fully trained at appropriate levels per ARMY and MEDCOM guidelines to provide system administration duties
- f. Provide around the clock monitoring and repair of system operations.
- g. Implement approved and planned changes to the LANs and document configuration changes.
- h. Provide security management in include scanning of server environment for vulnerabilities on a monthly basis
- i. Provide change management by tracking all changes to the server hardware in an Online Server Log.

Receiver will:

- a. Make requirements known to Supplier.
- b. Request services and support by providing necessary request and or documentation.
- c. Alert the Supplier as soon as possible on issues or problems that arise.
- d. Provide the Supplier all hardware and software requirements to satisfy request.
- e. Provide the Supplier documentation referencing any future, and anticipated hardware and Software upgrades.
- f. Provide the Supplier hardware and software maintenance.
- g. Provide the Supplier non-standard software administration training and documentation.
- h. Provide the Supplier twenty-four hours to restore user data
- i. Use single network server storage and all its components for official Government business only.

Single Use Server Hosting-Level 3

Description of Services: Fort Detrick DOIM provides server-hosting support for Single Use Servers. These servers contain programs that collectively serve the needs of the entire organization, a single user, department, or specialized application. These servers are provided to the DOIM by the customer. The customer is responsible for hardware and software maintenance on these servers. The DOIM can obtain maintenance for the customer on a reimbursement basis. In this usage, a server is both the computer hardware and its main software, the operating system. Monitoring and support are provided on a 7 x 24 coverage with after hours on call staff in the event of an outage. Scheduled maintenance will be performed within the window of 8:00-12:00 am EST on Sundays.

Supplier will:

- a. Provide Server Hosting services on dedicated servers on-site at Fort Detrick DOIM Building 1422 (administration, back-up, and data storage) to include:
- b. Monitor, coordinate and administer server resources.
- c. Maintain the availability of the server(s) to its users.
- d. Advise and assist users regarding access to the server(s).
- e. Establish and perform system backup procedures and documentation to include storage of backup media and DR drives at a remote COOP site.
- f. Provide technical staff that are fully trained at appropriate levels per ARMY and MEDCOM guidelines to provide system administration duties
- g. Implement a comprehensive information security program per AR25-2, ARMY and MEDCOM guidelines and physical security procedures.
- h. Use fault management techniques designed to diagnose problems and provide timely solutions.
- i. Monitor the user environment, including login scripts, menu creation, and directory structure, as needed.
- j. Perform regularly scheduled evaluation and maintenance of all components (i.e. file servers, and print servers), including preventive maintenance.
- k. Provide around the clock monitoring and repair of system operations.
- l. Implement approved and planned changes to the LANs and document configuration changes.
- m. Provide security management include scanning of server environment for vulnerabilities on a monthly basis
- n. Provide change management by tracking all changes to the server hardware in an Online Server Log.
- o. Inform the user community of any planned maintenance or outage schedules that will impact the servers availability.

FY 2006
Supplier and Receiver Clauses

Receiver will:

- a. Make requirements known to Supplier.
- b. Request services and support by providing necessary request and or documentation.
- c. Alert the Supplier as soon as possible on issues or problems that arise.
- d. Provide the Supplier all hardware and software requirements to satisfy request.
- e. Provide the Supplier documentation referencing any future, and anticipated hardware and software upgrades.
- f. Provide the Supplier hardware and software maintenance.
- g. Provide the Supplier non-standard software administration training and documentation.
- h. Provide the supplier with appropriate pertinent information necessary when requesting new user account.
- i. Provide the Supplier twenty-four hours to restore user data.
- j. Use single network server storage and all its components for official Government business only.

FY 2006
Supplier and Receiver Clauses

E-Server

Description of Services: Fort Detrick DOIM provides an eServer as an application hosting platform. The eServer provides hosting of applications that serve the needs of specific customers on Ft Detrick. This platform is validated to a security Level B4 (i.e. suitable for critical applications and highly sensitive data) utilizing Resource Access Control Facility (RACF). The DOIM provides the following services: software upgrades, hardware maintenance, capacity management, backup and recovery services and full technical support—so that our customers' applications can run smoothly and deliver important services to their users.

Supplier will:

- a. Provide Resource Access Control Facility (RACF) security on platform
- b. Provide maintenance and backup of user files
- c. Off site storage for critical data
- d. Comprehensive change management
- e. 24x7 system monitoring and problem resolution
- f. User access to eServer
- g. Monitor, coordinate and administer eServer resources
- h. Maintain interfaces to support customer application enhancements. Insure interface files are transferred correctly and on a timely basis.
- i. Provide security on customer unique systems by assigning users to application groups, roles, and/or access to data files.

Receiver will:

- a. Make requirements known to Supplier
- b. Request services and support by providing necessary request and or documentation
- c. Receiver will notify the Supplier as soon as possible on issues or problems that arise
- d. Receiver will provide Supplier with 24 hours notice for a restore
- e. Review quarterly statements of usage to verify storage and job usage

Customer Support Center (CSC) Services

Description of Services: The CSC provides Information Technology (IT) support to end users of office automation tools. The CSC team provides Help Desk Services and Technical Support Services (also called Touch Labor) for end user devices to include desktop and laptop computers, Personal Digital Assistants (PDAs), printers, scanners, and other hardware (HW) as well as the software (SW) associated with these devices. The CSC's hours of operation are 0700 – 1700 EST Monday through Friday. However, outside of these hours, and on weekends and holidays, calls to the CSC are forwarded to the USAG DOIM Data Center. Data Center personnel are not responsible for direct problem resolution but instead are responsible for escalating calls to the appropriate on-call personnel. The addition of this service provides customers with 24 X 7 access to technical support services. CSC support is available via phone, fax, email, and voicemail. The CSC offers varying levels of standard services that are available by subscription or direct reimbursement. Below are the descriptions of CSC services.

Help Desk Services

Direct Support – Subscribers to this level of support use the CSC Help Desk as the primary recipient of customer calls. This level of service includes support for the full range of standard IT assets and access to the full range of technical support services. This includes nominal hardware replacement for items not under warranty and the coordination of warranty services for items under a manufacturer's warranty. In providing these services, the Help Desk's support strategy is in line with industry best practices and seeks to resolve customer's problems at the first level of contact. In addition, the Help Desk is responsible for retaining call ownership until the customer's problem is resolved. This ensures that the Help Desk never loses sight of a customer's request. The Help Desk manages problem resolution through various priority and support levels.

General Support – Subscribers to this level of support use the DOIM Help Desk as the secondary recipient of customer calls. That is, the customer has access to internal or other helpdesk support and this support is used prior to contacting the DOIM helpdesk. However, once contacted, the Help Desk provides the same services listed above under Direct Support Services.

Administrative Services (Non-Technical) – Included in the services listed above are those non-technical services that may support customers directly or indirectly by providing assistance to internal technical support personnel. These services generally include but are not limited to: sending, receiving, and analyzing customer satisfaction surveys; preparation of ad hoc and standard reports; Customer Relationship Management (CRM); maintenance and sustainment of CSC Hardware and Software tools (Automatic Call Distributor, HEAT, Business Rule Monitor, etc.) collection and reporting of performance data (metrics); and process analysis and improvement.

FY 2006
Supplier and Receiver Clauses

Dedicated Support – The CSC can provide full or part-time Technical Support personnel dedicated to providing on-site customer support. Customers can specify the duration, level and type of IT support required from Tier I up to a Senior Tier II technician. The cost of these services is dependent on the level of effort, the skill level of the technician, and the type of IT support requested. Pricing for these services is provided on a case-by-case basis and funding is via direct reimbursement.

Non-standard Hardware/Software Support – Occasionally, customers may obtain IT assets that are significantly different from the assets normally supported by the Customer Support Center. Since it is possible that CSC technicians would require additional training in order to support such assets, pricing for these services is provided on a case-by-case basis and funding is via direct reimbursement.

Subject Matter Expert (SME) Services (Technical) – The CSC also offers ad hoc support on an as requested basis. This support typically involves the use of an individual or groups with specific technical knowledge and expertise regarding a particular product or service. These services are generally consultative in nature and can cover a wide range of Information Technology areas including but not limited to: Help Desk Operations, Hardware and Software operations and maintenance; applications use, modification, and sustainment; and manufactures' recommendations regarding product use, upgrades, and sustainment. The cost of these services is dependent on the level of effort, the skill level of the personnel involved, and the type of IT support requested. Pricing for these services is provided on a case-by-case basis and funding is via direct reimbursement.

Customer Support Center (CSC) MPMC Services

Description of Services: The CSC provides IT support to end users of office automation tools. The CSC team provides Help Desk Services and Technical Support Services (also called Touch Labor) for end user devices to include desktop and laptop computers, Personal Digital Assistants (PDAs), printers, scanners, and other hardware (HW) as well as the software (SW) associated with these devices. The CSC's hours of operation are 0600 – 1800 EST Monday through Friday. However, outside of these hours, and on weekends and holidays, calls to the CSC are forwarded to the USAG DOIM Data Center. Data Center personnel are not responsible for direct problem resolution but instead are responsible for escalating calls to the appropriate on-call personnel. The addition of this service provides customers with 24 X 7 access to technical support services. CSC support is available via phone, fax, email, and voicemail. The CSC offers varying levels of standard services that are available by subscription or direct reimbursement. Below are the descriptions of CSC services.

Help Desk Services

Direct Support – Subscribers to this level of support use the CSC Help Desk as the primary recipient of customer calls. This level of service includes support for the full range of standard IT assets and access to the full range of technical support services. This includes nominal hardware replacement for items not under warranty and the coordination of warranty services for items under a manufacturer's warranty. In providing these services, the Help Desk's support strategy is in line with industry best practices and seeks to resolve customer's problems at the first level of contact. In addition, the Help Desk is responsible for retaining call ownership until the customer's problem is resolved. This ensures that the Help Desk never loses sight of a customer's request. The Help Desk manages problem resolution through various priority and support levels.

Incoming calls are prioritized and attempts are made to resolve the problem at the lowest possible level. This level is referred to as Tier I. Tier I services include but are not limited to: receiving, logging, and tracking 100% of service requests until closure; answering 90% of phone inquiries within 45 seconds; checking voice mail inquiries within 30 minutes of the voice mail being placed; replying to 100% of email inquiries within 30 minutes of the email inquiry being sent; verifying and correcting customer contact information; attempting to resolve all calls at the Tier I level; and expeditiously elevating calls that are not able to be resolved at the Tier I level to the correct higher level support personnel. This support may be provided via remote desktop capabilities if available and if appropriate for use under the specific problem circumstances.

In the event a customer's problem cannot be resolved at the first level, the call is escalated to a second level of support, called Tier II. Tier II services are Technical Support services (also called Touch Labor) that include but are not limited to: the on-site services of Technical Support personnel that are

FY 2006
Supplier and Receiver Clauses

knowledgeable of the hardware, commercial off the shelf software, government software utilized by the receiving organization, and network architecture and operations. Technical personnel respond within the designated timeframes set out according to the designated priority and respond to trouble tickets and projects courteously and professionally. Technical Support personnel triage, document, and elevate un-closable trouble tickets expeditiously to Tier III, other Tier II, and/or outside support entities and document their efforts efficiently thoroughly, and accurately. This support may be provided via remote desktop capabilities if available and if appropriate for use under the specific problem circumstances.

In the event that the customer's problem still cannot be resolved at the Tier II level, a third level of support is available within the Fort Detrick DOIM. This level is called Tier III. Tier III technicians are the highest level of support available within the DOIM. Tier III services are typically provided by System and Database Administrators, Network Specialists, and personnel with advanced skills on a particular platform or application. Tier III services are also, on occasion, used by default for certain specific issues where it is understood that Tier III services will always be required. Tier III personnel also provide much of the non-duty hour support and are generally the ones in an on-call status.

Administrative Services (Non-Technical) – Included in the services listed above are those non-technical services that may support customers directly or indirectly by providing assistance to internal technical support personnel. These services generally include but are not limited to: sending, receiving, and analyzing customer satisfaction surveys; preparation of ad hoc and standard reports; Customer Relationship Management (CRM); maintenance and sustainment of CSC Hardware and Software tools (Automatic Call Distributor, HEAT, Business Rule Monitor, etc.) collection and reporting of performance data (metrics); and process analysis and improvement.

Dedicated Support – The CSC can provide full or part-time Technical Support personnel dedicated to providing on-site customer support. Customers can specify the duration, level and type of IT support required from Tier I up to a Senior Tier II technician. The cost of these services is dependent on the level of effort, the skill level of the technician, and the type of IT support requested. Pricing for these services is provided on a case-by-case basis and funding is via direct reimbursement.

Non-standard Hardware/Software Support – Occasionally, customers may obtain IT assets that are significantly different from the assets normally supported by the Customer Support Center. Since it is possible that CSC technicians would require additional training in order to support such assets, pricing for these services is provided on a case-by-case basis and funding is via direct reimbursement.

FY 2006
Supplier and Receiver Clauses

Subject Matter Expert (SME) Services (Technical) – The CSC also offers ad hoc support on an as requested basis. This support typically involves the use of an individual or groups with specific technical knowledge and expertise regarding a particular product or service. These services are generally consultative in nature and can cover a wide range of Information Technology areas including but not limited to: Help Desk Operations, Hardware and Software operations and maintenance; applications use, modification, and sustainment; and manufactures' recommendations regarding product use, upgrades, and sustainment. The cost of these services is dependent on the level of effort, the skill level of the personnel involved, and the type of IT support requested. Pricing for these services is provided on a case-by-case basis and funding is via direct reimbursement.

Patch Management

Description of Services: The DOIM will provide patch management services utilizing patch management tools to include Microsoft's System Managed Server (SMS) and other automated patch management tools to support to all Windows computers to include software distribution. These patch management products provide efficient levels of support to reduce "touch labor" as well as providing asset management, remote troubleshooting, security updates, reports on inventories, software metering, and Windows-based management.

Supplier Will:

- a. Push IAVA's and security patches to desktops under the DOIM control as required to meet MEDCOM and Army guidelines
- b. Push software applications, software application updates (service packs and hotfixes) as required
- c. Upon request/need, develop and run reports of unauthorized software
- d. Monitor desktop license metering
- e. Provide remote troubleshooting capability
- f. Provide standard web-based reports or customized reports based upon the customers requirements

Receiver Will:

- a. Adherence to standard software list available from the DOIM
- b. Responsible for reading pop-up informational messages and notices
- c. Designate an internal point of contact within the customer's organization for trouble shooting purposes on agent workstations, participating in testing as required and coordinating times for software pushes.

Secret Internet Protocol Router NETwork (SIPRNET)

Description of Services: Fort Detrick DOIM provides Fort Detrick customers with access to the SIPRNET.

Support provided by other activities at Fort Detrick is as follows...

- a. The 302d Signal BN houses the Point of Presence (POP), located in building 1671, which services a T-1 (1.5Mbps) connection. The 302d Signal BN provides keying and troubleshooting support for all crypto equipment.
- b. The Information Systems Engineering Command-Fort Detrick Engineering Division (ISEC-FDED) is contactor for engineering, installation and initial operational capability for all SIPRNET activities at Fort Detrick. The ISEC-FDED also serves as the Configuration Control Board (CCB) for the Fort Detrick SIPRNET.

Supplier will:

- c. Provide access to the SIPRNET WAN
- d. Ensure that antivirus products are kept up to date
- e. Ensure that IAVA procedures and implementation processes are applied to all SIPRNET connected devices, excluding crypto gear, as identified through the current Army IAVA message dissemination procedures (ACERT LISTSERVER).
- f. Perform Harris Stat security scans, as necessary, after appropriate coordination with the SIPRNET community.
- g. Develop and maintain the DITSCAP for the Fort Detrick SIPRNET customers
- h. Troubleshoot and maintain the SIPRNET network for Fort Detrick

Receiver will:

- a. Maintain physical and personnel security in accordance with DITSCAP SSAA
- b. Provide necessary funding to the DOIM
- c. Request services and support by providing necessary request and/or documentation
- d. Notify the Supplier by contacting the Fort Detrick Help Desk at 301-619-2049 as soon as possible on issues or problems as they arise.
- e. Provide the Supplier 48 hours advance notice when requesting additional support outside standard business hours.

SQL/FileMaker Applications

Description of Services: U.S. Army Garrison, Fort Detrick provides technical management support for maintenance of SQL/FileMaker Pro web applications. The technical administrators assist developers with development of interface scripts, database problems, implementation of database modifications, interfaces with other operational systems, capacity planning, application upgrades, migration of objects from development to test and test to production, database change management, and migration to new hardware and operating system upgrades.

Supplier will:

- a. Perform analysis and design work associated with development, implementation, and maintenance of logical databases: database designs that support the transformation of business requirements into logical and physical databases.
- b. Provide ongoing support of the DBMS environments and work closely with customers and application support team to resolve support issues.
- c. Monitor interface file transfers, database performance, storage/space requirements, and recommend/implement enhancements.
- d. Research, analyze, recommend and implement new technologies, standard processes, tools and techniques.
- e. Design, build and populate database table structures to support project development.
- f. Install, configure, administer, and maintain databases.
- g. Monitor and tune DBMS and application program performance.
- h. Monitor, coordinate and administer SQL/FileMaker Pro server resources
- i. Maintain interfaces to support current DOD/Army application enhancements. Insure interface files are transferred correctly and on a timely basis.
- j. Provide security on unique systems by assigning users to application groups, roles, and/or access to data files.
- k. Provide backup and recovery of databases and applications, and troubleshoot technical problems.
- l. Works with application service owners to plan down time tolerance for backups/recoveries, application upgrades, and database software upgrades/maintenance.
- m. Schedule running of database integrity utilities, monitor results, and address database inconsistencies.
- n. Assist in the product testing and selection of all tools related to database administration.
- o. Implement server/database security, assign users to data server groups, create system and server logins, add users to databases, assign server roles, and set permissions on database objects.

FY 2006
Supplier and Receiver Clauses

SQL Applications supported are:

SFQ-Web (Stanfins Query), PIRS-Web (Permits and Inspection Requirements System), AVIS-Web (Audio Visual Information System), EMTS (Executive Management Tracking System).

Starting FY06: AIRS-Web (Automated Integrated Requirements System, AAS-Web (Automated Acquisition System, AIRS/SPS Adaptor Interfaces),

FileMaker Pro Applications supported are:

USAG: Personnel System, Excess Property, Security Office

USAG-DOIM: Personnel System, IP Address list, Telephone Admin System, Telephone Cables System, Billing Statements (SLA info)

OTSG: Personnel System (in San Antonio and Skyline)

SiteR garrison: Excess Property

Receiver will:

- a. Make requirements known to Supplier
- b. Request services and support by providing necessary request and or documentation
- c. Receiver will notify the Supplier as soon as possible on issues or problems that arise
- d. Provide the Supplier documentation referencing any future, and anticipated DBMS environment hardware/software upgrades
- e. Receiver will provide the Supplier 48 hours advance notice when requesting additional support outside standard business hours
- f. Provide the Supplier with appropriate pertinent information necessary when requesting new DBMS account
- g. Receiver will notify Supplier immediately when a user departs or changes duty station in order to remove user account from the DBMS environment
- h. Provide the Supplier advance notice to restore DBMS data.

***Automated Time Attendance and Production System
(ATAAPS Support)***

Description of Services: FORT DETRICK DOIM provides support for the ATAAPS application. ATAAPS provides an automated, single-source input for reporting and collecting time and attendance (T and A) data. Thru a partnership between customers and the Fort Detrick DOIM, employee records and accounting data is imported from DFAS and automatically posted to the database. Database management/changes and application software changes downloaded from DFAS and installed by the DOIM, collectively serves the need of organizations using this application. The DOIM is the primary technical POC concerning ATAAPS database, system administration, network, release management, and communication issues.

Supplier will:

- a. Install, configure, administer, and maintain the ATAAPS database.
- b. Establish user accounts (or roles) for database access.
- c. Download and install Application Software changes.
- d. Download and install DataBase changes.
- e. Install new organization installation parameters, grant security authorization levels, populate database accounting-related data, and verify data created in the database during initial installation.
- f. Purge database historical information, edit “raw” data when necessary, and synchronize system numbers throughout the database.
- g. Assign user logon Ids and passwords and ensure users have proper access privileges to the database.
- h. Ensure proper security authorizations have been granted.
- i. Maintain Pay Period information.
- j. Maintain Holiday information.
- k. Monitor and tune DBMS and application program performance.
- l. Provide backup and recovery of databases and applications, and troubleshoot technical problems.
- m. Works with application service owners to plan down time tolerance for backups/ recoveries, application upgrades, and database software upgrades/maintenance.
- n. Schedule running of database integrity utilities, monitor results, and address database inconsistencies.
- o. Monitor database performance and storage/space requirements.
- p. Maintain the availability of the server(s) to its users.
- q. Advise and assist users regarding access to the server(s).
- r. Implement physical security procedures.
- s. Diagnose problems and provide timely solutions.

FY 2006
Supplier and Receiver Clauses

- t. Monitor the user environment, including login scripts, and directory structure, as needed.
- u. Perform regularly scheduled evaluation and maintenance of all components (i.e. file servers, and print servers), including preventive maintenance.
- v. Provide around the clock monitoring and repair of system operations.

Receiver will:

- a. Make requirements known to Supplier
- b. Request services and support by providing necessary request and or documentation
- c. Alert the Supplier as soon as possible on issues or problems that arise
- d. Provide the supplier with appropriate pertinent information necessary when requesting new user account
- e. Notify the supplier immediately when a user departs or changes duty station in order to remove any data referencing user account
- f. Receiver will provide the Supplier 48 hours advance notice when requesting additional support outside standard business hours
- g. Provide the Supplier with appropriate pertinent information necessary when requesting new DBMS account

Web Services – Level 1 Site Hosting

Description of Services: Web hosting consists of a group of tasks that apply to all web sites and are performed in support of Fort Detrick DOIM web farm maintenance, web server security, and assurance of compliance with applicable federal and DoD regulations and guidance. Fort Detrick DOIM has implemented 3 (three) levels of hosting. Fort Detrick DOIM provides core services that are then applied to one of three hosting levels. The core hosting deliverables and services offered to receiver - include non-operating system (OS) server application support, OS server application support, OS security, access control, fire wall access and controls, virus protection, data backups, DNS registration, DoD/OPSEC web server compliance, redundancy support, 24x7 operational support, growth capacity, Web domain architecture, internal PD coordination/monitoring, and WebTrends quarterly reporting.

Supplier will:

- a. Provide up to 25 MB disk space.
- b. Provide live server.
- c. Provide review server.
- d. Provide staging server.
- e. Provide domain controller.
- f. Provide all core services.
- g. Provide access to the following Web applications:
 - HTML

Receiver will:

In order to help facilitate web site sustainability, it is crucial to have customer involvement. Therefore, the Receiver is expected to:

- a. Provide functional requirements.
- b. Provide content manager designation.
- c. Provide related documentation.
- d. Provide compliance authorization.

Web Services – Level 2 Site Hosting

Description of Services: Web hosting consists of a group of tasks that apply to all web sites and are performed in support of Fort Detrick DOIM web farm maintenance, web server security, and assurance of compliance with applicable federal and DoD regulations and guidance. Fort Detrick DOIM has implemented 3 (three) levels of hosting. Fort Detrick DOIM provides core services that are then applied to one of three hosting levels. The core hosting deliverables and services offered to receiver - include non-operating system (OS) server application support, OS server application support, OS security, access control, fire wall access and controls, virus protection, data backups, DNS registration, DoD/OPSEC web server compliance, redundancy support, 24x7 operational support, growth capacity, Web domain architecture, internal PD coordination/monitoring, and WebTrends quarterly reporting.

Supplier will:

- a. Provide 25 MB to 99 MB disk space.
- b. Provide live server.
- c. Provide review server.
- d. Provide staging server.
- e. Provide domain controller.
- f. Provide all core services.
- g. Provide access to the following Web applications:
 - Cold Fusion MX
 - Cold Fusion Verity Search Engine
 - ASP
 - ASP.NET
 - Multimedia and other related support

Receiver will:

In order to help facilitate web site sustainability, it is crucial to have customer involvement. Therefore, the Receiver is expected to:

- Provide functional requirements.
- Provide content manager designation.
- Provide related documentation.
- Provide compliance authorization.

Web Services – Level 3 Site Hosting

Description of Services: Web hosting consists of a group of tasks that apply to all web sites and are performed in support of Fort Detrick DOIM web farm maintenance, web server security, and assurance of compliance with applicable federal and DoD regulations and guidance. Fort Detrick DOIM has implemented 3 (three) levels of hosting. Fort Detrick DOIM provides core services that are then applied to one of three hosting levels. The core hosting deliverables and services offered to receiver - include non-operating system (OS) server application support, OS server application support, OS security, access control, fire wall access and controls, virus protection, data backups, DNS registration, DoD/OPSEC web server compliance, redundancy support, 24x7 operational support, growth capacity, Web domain architecture, internal PD coordination/monitoring, and Web Trends quarterly reporting.

Supplier will:

- a. Provide 100 MB+ disk space.
- b. Provide live server.
- c. Provide review server.
- d. Provide staging server.
- e. Provide domain controller.
- f. Provide all core services.
- g. Provide access to the following Web applications:
 - Cold Fusion MX
 - Cold Fusion Verity Search Engine
 - ASP
 - Multimedia and other related support
- h. Provide full access to Database Support:
 - Microsoft SQL
 - Oracle

Receiver will:

In order to help facilitate web site sustainability, it is crucial to have customer involvement. Therefore, the Receiver is expected to:

- a. Provide functional requirements.
- b. Provide content manager designation.
- c. Provide related documentation.
- d. Provide compliance authorization.

Web Services – Other (WEB Development)

Description of Services: Fort Detrick DOIM provides a full suite of web services. The management and technical support includes approaches that address full cradle-to-grave solutions. These solutions include: DoD compliant products; configuration management; content management; requirements analysis; systems architecture; phased implementation and hosting; risk mitigation; cost controls; performance monitoring; and in-progress reviews.

Web Hosting - Fort Detrick DOIM understands that each client's web hosting requirements are very diverse, so Fort Detrick DOIM's hosting platform is engineered to provide the upmost flexibility to meet virtually any hosting requirement. Fort Detrick DOIM provides 24x7 operational support, fully compliant (DoD, U.S. Army, OPSEC, and PKI) web services, configuration management, phased implementation, risk mitigation, performance monitoring, database and other server software application support including many unique applications on our DITSCAP approved web hosting facility. Our technical approach to web hosting includes the following major steps - determination of development and hosting criteria for the web site; determination of system architecture and infrastructure requirements to achieve required web site capabilities and functionality; test and integrate web site into system architecture and infrastructure; ensure web site content meets all compliance requirements; review web site content data with customer for approval and host and maintain live web sites.

Web Design - Fort Detrick DOIM designs and develops web sites capturing high visual aesthetics and functionality while complying with all Federal, DoD, and U.S. Army web policies, regulations and guidance (e.g., PKI, Section 508 – ADA, security and access control and information security). Web site design and development starts by capturing detailed site requirements through a partnership between the client and Fort Detrick DOIM. The site requirements are then analyzed and Fort Detrick DOIM's web site design and development is applied to create a finished solution.

Supplier will:

- a. Offer full service hosting and administration of Internet/Intranet Web sites.
- b. Offer DoD, Operational Security (OPSEC) and PKI compliant Web services.
- c. Offer access control, intrusion monitoring and virus protection.
- d. Offer data backup and data restoration.
- e. Offer 24x7 operational support.
- f. Offer a multitude of supported applications including: Oracle, SQL, ColdFusion, ASP and more.
- g. Offer Web page development.
- h. Offer robust Web site designs and scalable solutions.

FY 2006
Supplier and Receiver Clauses

- i. Offer customer-oriented site development.
- j. Offer enhanced professional graphics.
- k. Offer Web design and development Subject Matter Experts.
- l. Provide Content Management.
- m. Offer DoD compliant Web services.

Receiver will:

- a. Provide functional requirements.
- b. Provide content manager designation.
- c. Provide any related documentation.
- d. Provide compliance authorization.

Customer Account Manager (CAM) and Project Management Support

Description of Services: Fort Detrick DOIM provides full scope of LCM for Fort Detrick DOIM developed applications. These services include planning, acquisition, operation, maintenance, and replacement of IT assets and services. Fort Detrick DOIM can provide Project Management Support based on industry and government best practices. The services are reimbursable based on a requirements analysis and the terms of a written agreement (i.e. proposal) between Fort Detrick DOIM and the customer.

Supplier will:

- a. Review IT purchase requests for configuration and standards compliance.
- b. Establish guidelines for the acquisition and life cycle replacement of all automation equipment

Receiver will:

- a. Make requirements known to CAM
- b. Request services and support by providing necessary request and or documentation
- c. Receiver will alert the CAM as soon as possible on issues or problems that arise
- d. Receiver will provide the supplier with appropriate pertinent information necessary.
- e. When requesting new IT purchases.

Application Support for General Use and Legacy Systems (ISMs)

Description of Services: Fort Detrick DOIM provides application support for maintenance of Department of Defense Installation Support Modules (ISMs), Standard Army Management Information Systems (STAMIS), DoD/Army approved interfaces, and Detrick unique applications that support customers post-wide. The Program Executive Office, Standard Army Management Information Systems (PEO STAMIS), performs as the Army centralized manager for assigned programs reporting, through the DISC4, to the Army Acquisition Executive (AAE). The PEO STAMIS provides overall direction and guidance for the development, acquisition testing, product improvement, and fielding of assigned programs. The PEO coordinates, integrates, leads, and directly controls the Program/Project Managers (PMs) within the standard Army management information systems mission area, placing primary emphasis on cost estimating, planning, programming, budgeting, program integration, interoperability, and oversight. Support also includes application development, technical consultation, and providing system requirements, system specifications, and user guide technical documentation.

Supplier will:

- a. Fort Detrick DOIM will provide Fort Detrick customers with support for the applications listed below. This support includes maintenance of DOD ISM and ARMY STAMMIS systems. It also includes analysis and design, development, implementation, maintenance, and documentation support for the Detrick unique systems that support customers post-wide.
- b. Assist in testing and selection of tools related to application support.
- c. Provide security on Detrick unique systems by assigning users to application groups, roles, and/or access to data files.
- d. Maintain/modify existing ISM/STAMMIS interfaces to support current DOD/Army application enhancements. Insure interface files are transferred correctly and on a timely basis.
- e. Support installation level, DA and DoD standard systems designated for centralized installation support. IAW established Installation Computer System Configuration Baseline (CSCB)
- f. Applications Supported:

AcqPro (Acquisition Professional for SOW and SOPs)	FAS (Fire Alarm Sys)	SECCLEAR ISM	DAMIS (Drug & Alcohol Management Info Sys) ISM	NAF-D ISM	USAG Excess Property / Inventory
AFMIS (Army Food Management Info Sys) ISM	HIS (Heat Index Sys)	STANFINS (Standard Army Financial Sys) ISM	DCAS (Direct Commitment Accounting Sys) Interface	OUTPROC (Military Out Processing Sys) ISM	USAG Pers TDA

FY 2006
Supplier and Receiver Clauses

AMEDDPAS ISM	INPROC (Military In Processing) ISM	TMS (Tel Mgmt Sys)	DCPS ISM	PERSLOC (Personnel Location Sys) ISM	USS (USAG Security Sys)
ATAAPS (Automated Time, Attendance & Production Sys)	Lending Closet	TRANSPROC (Transition Point Processing) ISM	DENTRAD (DoD Dental Readiness Program) ISM	PTD (Post Telephone Directory)	Intergraph
AVIS (Audio Visual Sys)	MILPO ISM	TSAMS-E ISM	DTS-L (Defense Travel Sys – Limited)	RECTRAC ISM	Safety ISM
CYLIVE	MSDS (Material Safety Data Sheets)	UKS (USAG Key Sys)	EDMIS (Education Management Sys) ISM		

Receiver will:

- a. Make requirements known to Supplier
- b. Request services and support by providing necessary request and or documentation
- c. Receiver will notify the Supplier as soon as possible on issues or problems that arise
- d. Receiver will provide the Supplier 48 hours advance notice when requesting additional support outside standard business hours.

DBA Support - Oracle

Description of Services: U.S. Army Garrison, Fort Detrick provides database management support for maintenance of legacy applications, Department of Defense Installation Support Modules (ISM) and Commercial Off-the-Shelf (COTS) software. The DBAs assists developers with database problems, implementation of database modifications, interfaces with other operational systems, capacity planning, application upgrades, migration of objects from development to test and test to production, database change management, and migration to new hardware and operating system upgrades.

Supplier will:

- a. Perform analysis and design work associated with development, implementation, and maintenance of logical databases: database designs that support the transformation of business requirements into logical and physical databases.
- b. Provide ongoing support of the DBMS environments and work closely with customers and application support team to resolve support issues.
- c. Monitor database performance, storage/space requirements, and recommend/implement enhancements.
- d. Research, analyze, recommend and implement new technologies, standard processes, tools and techniques.
- e. Design, build and populate database table structures to support project development.
- f. Install, configure, administer, and maintain databases.
- g. Monitor and tune DBMS and application program performance.
- h. Provide backup and recovery of databases and applications, and troubleshoot technical problems.
- i. Works with application service owners to plan down time tolerance for backups/recoveries, application upgrades, and database software upgrades/maintenance.
- j. Schedule running of database integrity utilities, monitor results, and address database inconsistencies.
- k. Assist in the product testing and selection of all tools related to database administration.
- l. Implement server/database security, assign users to data server groups, create system and server logins, add users to databases, assign server roles, and set permissions on database objects.
- m. Install Oracle security patches to protect databases and applications.

Receiver will:

- a. Make requirements known to Supplier

FY 2006
Supplier and Receiver Clauses

- b. Request services and support by providing necessary request and or documentation
- c. Receiver will notify the Supplier as soon as possible on issues or problems that arise
- d. Provide the Supplier documentation referencing any future, and anticipated DBMS environment hardware/software upgrades
- e. Receiver will provide the Supplier 48 hours advance notice when requesting additional support outside standard business hours
- f. Provide the Supplier with appropriate pertinent information necessary when requesting new DBMS account
- g. Receiver will notify Supplier immediately when a user departs or changes duty station in order to remove user account from the DBMS environment
- h. Provide the Supplier advance notice to restore DBMS data.